Vendor Landscape: Security Information & Event Management (SIEM)

Optimize IT security management and simplify compliance with SIEM tools.

Info-Tech Research Group, Inc. Is a global leader in providing IT research and advice.
Info-Tech's products and services combine actionable insight and relevant advice with
ready-to-use tools and templates that cover the full spectrum of IT concerns.

INFO~TECH
RESEARCH GROUP

Introduction

Understand your organization's requirements for Security Information & Event Management (SIEM) to ensure product selection achieves key goals.

This Research Is Designed For:

✓Organizations seeking a SIEM solution.

✓Their SIEM use case may include:

- IT leaders considering SIEM technology to reduce the cost of meeting ever-increasing compliance requirements.
- IT leaders looking to enhance the effectiveness of existing IT security operations.
- Organizations seeking to improve risk management processes.

This Research Will Help You:

✓Understand the capabilities of SIEM technologies and their potential use cases.

✓Differentiate between vendor offerings and identify what aligns with your organization's requirements.

✓Shortlist vendors, prepare a request for proposal (RFP), and score RFP responses to select a SIEM solution.

✓Maximize your investment in SIEM.

Executive summary

Info-Tech evaluated ten competitors in the SIEM market, including the following notable performers:

Champions:

- **LogRhythm,** a strong advanced feature offering enables this dedicated SIEM vendor to be a champion in this VL.
- **RSA,** one of the most respected and recognized security vendors, offers a high security SIEM product.

Value Award:

- **TIBCO,** a strong player with more to come, TIBCO is developing its security analytics offering while remaining at a lower price point.

Trend Setter Award:

- **RSA** deployed a new commercial breed of SIEM consisting of multiple platforms across aggregation, normalization, and analysis to provide stronger threat detection.

Info-Tech Insight

1. **Scalable management:**

   Organizations need to know the scalable level of SIEM they require. Less competent security organizations should adopt full out-of-the box solutions. High security demand organizations can purchase larger SIEM vendor solutions that are often a component of larger security suites offering operations management, analytics, and incident management.

2. **Powerful analytic tools:**

   As targeted attacks and persistent adversaries advance, advanced correlation capabilities and the ability to detect suspicious activity from less data and varied data becomes more important.

3. **Data sources:**

   A SIEM needs as many sources as possible. Long-term data event and context retention with analytics, in addition to threat intelligence feeds, can provide a differentiating factor over standard log collection.

Market overview

How it got here

- Originally, basic log centralization was created from a need for central review capabilities. Regulatory and compliance requirements began to take effect requiring certain controls, including monitoring of logs, to be part of an organization's information security.
- SIEM grew from the conjoining Security Event Management and Security Information Management (which itself grew out of simpler Log Management).
- The market soon needed increased detection capabilities. From log collection moving into SIEM functions, threat detection and intelligence tools were developed to provide network visibility.
- SIEM solutions historically focused on large, regulated enterprises. Today vendors offer simplified, streamlined, all-in-one solutions aimed at the SME space.
- SIEM technologies are adapting to increased demand for a variety of offerings while developing better detection capabilities in the face of targeted attacks.

Where it's going

- Vendors will improve threat intelligence gathering and feeding capabilities to decrease time to detect the latest threats. As well, an increased focus on security analytics will emerge to detect targeted attacks based on small data volumes.
- SME customers will increase demand for full out-of-the-box SIEM solutions that are easy to use with near-full feature functions and support services.
- Increasing consolidation is occurring in the market with larger security vendors or infrastructure firms purchasing dedicated SIEM organizations. This may result in decreasing competitive evaluations by customers if they are concerned with seeking a strategic vendor.
- Managed SIEM services will take on increasing importance as smaller or less inclined organizations seek out third-party support to monitor SIEM on a continuous basis.
- The ability for the product to learn to recognize what's abnormal (adaptive intelligence) will become a differentiating factor once it is developed commercially.

Info-Tech Insight

As the market evolves, capabilities that were once cutting edge become default and new functionality becomes differentiating. Log data enrichment has become a Table Stakes capability and should no longer be used to differentiate solutions. Instead focus on peripheral security solution integration and security analytic capabilities to get the best fit for your requirements.

SIEM vendor selection / knock-out criteria: market share, mind share, and platform coverage

- SIEM solutions need to aggregate machine data in real time for risk management through analysis and correlation to provide network event monitoring, user activity monitoring, compliance reporting, as well as store and report data for incident response, forensics, and regulatory compliance.
- For this Vendor Landscape, Info-Tech focused on those vendors that offer broad capabilities across multiple platforms and that have a strong market presence and/or reputational presence among mid and large sized enterprises.

Included in this Vendor Landscape:

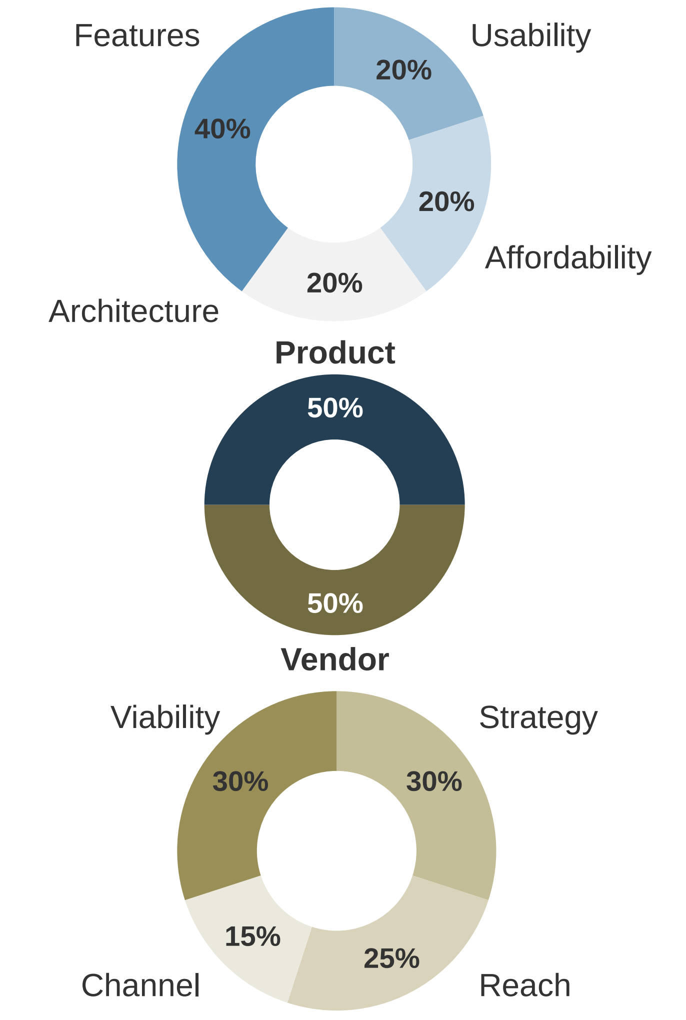
- **HP.** One of the largest vendors supports the most feature-rich SIEM solutions in this VL.
- **IBM.** IBM provides strong event and log management and threat detection across networks and applications.
- **LogRhythm.** As a dedicated vendor, LogRhythm offers a feature-rich product with the ability to adapt to trends.
- **McAfee (Intel).** A diverse and competitive vendor, McAfee offers a stable and reliable SIEM product.
- **NetIQ.** A subsidiary of a software holding company, NetIQ has a solid SIEM offering.
- **RSA.** RSA offers a highly advanced SIEM product garnered to large-scale, high-demand security organizations.
- **SolarWinds.** SolarWinds offers strong compliance and overall threat management functionality.
- **Splunk.** As a big data software company, Splunk lends itself well to the SIEM landscape.
- **TIBCO.** TIBCO, a security firm specializing in cloud protection through on-premise deployment, has a strong product.
- **Trustwave.** Entering the market through acquisition, Trustwave specializes in PCI compliance and managed services.

SIEM criteria & weighting factors

Product Evaluation Criteria	
Features	The solution provides basic and advanced feature/functionality.
Usability	The end-user and administrative interfaces are intuitive and offer streamlined workflow.
Affordability	Implementing and operating the solution is affordable given the technology.
Architecture	Multiple deployment options and extensive integration capabilities are available.

Vendor Evaluation Criteria	
Viability	Vendor is profitable, knowledgeable, and will be around for the long term.
Strategy	Vendor is committed to the space and has a future product and portfolio roadmap.
Reach	Vendor offers global coverage and is able to sell and provide post-sales support.
Channel	Vendor channel strategy is appropriate and the channels themselves are strong.

Criteria Weighting



The Info-Tech SIEM Vendor Landscape

The zones of the Landscape

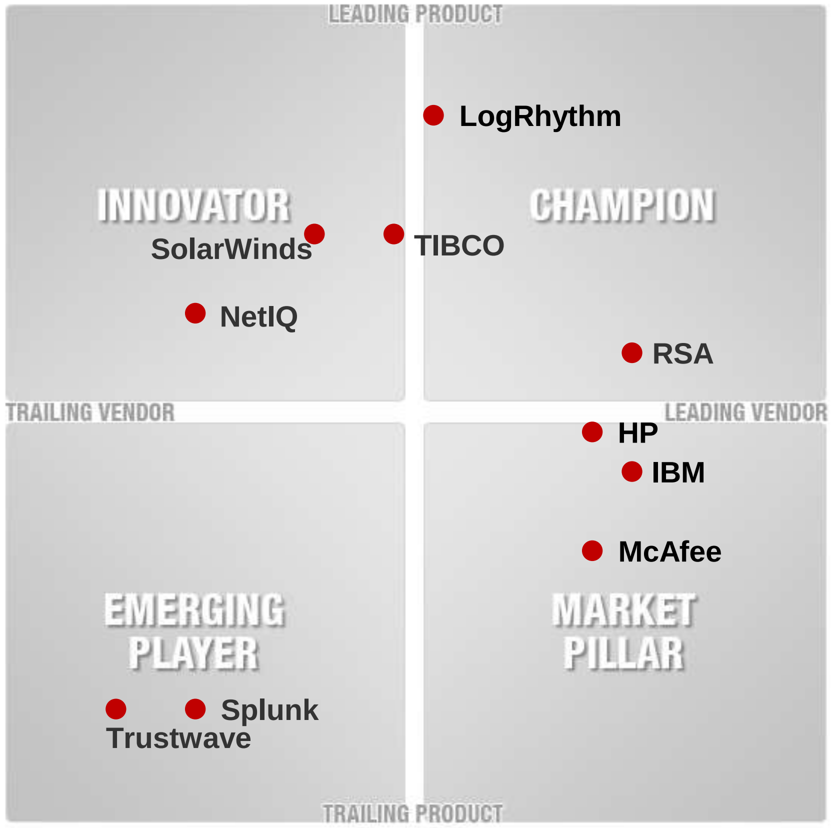
Champions receive high scores for most evaluation criteria and offer excellent value. They have a strong market presence and are usually the trend setters for the industry.

Market Pillars are established players with very strong vendor credentials, but with more average product scores.

Innovators have demonstrated innovative product strengths that act as their competitive advantage in appealing to niche segments of the market.

Emerging Players are comparatively newer vendors who are starting to gain a foothold in the marketplace. They balance product and vendor attributes, though score lower relative to market Champions.

The Info-Tech SIEM Vendor Landscape



For an explanation of how the Info-Tech Vendor Landscape is created, see Information Presentation – Vendor Landscape in the Appendix.

Balance individual strengths to find the best fit for your enterprise

	Product					Vendor				
	Overall	Features	Usability	Afford.	Arch.	Overall	Viability	Strategy	Reach	Channel
HP*	◕	●	◕	○	●	◕	●	◕	◕	●
IBM	◕	◕	◕	◔	●	●	●	◑	●	●
LogRhythm	●	●	●	◕	●	◕	◕	●	◕	◕
McAfee*	◑	◕	◕	○	◕	◕	●	◕	◕	◕
NetIQ	◕	●	◑	◕	◕	◕	◑	◕	◕	◕
RSA	◕	●	●	◔	●	●	●	◕	●	◕
SolarWinds	◕	◕	◕	●	◕	◕	◕	●	◕	◕
Splunk*	◑	◕	◑	○	◑	◕	◕	◑	◕	◕
TIBCO	●	◕	◕	●	●	◕	◕	◕	◕	◕
Trustwave*	◑	◕	◑	○	◕	◑	◕	◑	◕	◕

Legend ● **=Exemplary** ◕ **=Good** ◑ **=Adequate** ◔ **=Inadequate** ○ **=Poor**

*The vendor declined to provide pricing and publicly available pricing could not be found.

For an explanation of how the Info-Tech Harvey Balls are calculated, see Information Presentation – Criteria Scores (Harvey Balls) in the Appendix.

The Info-Tech SIEM Value Index

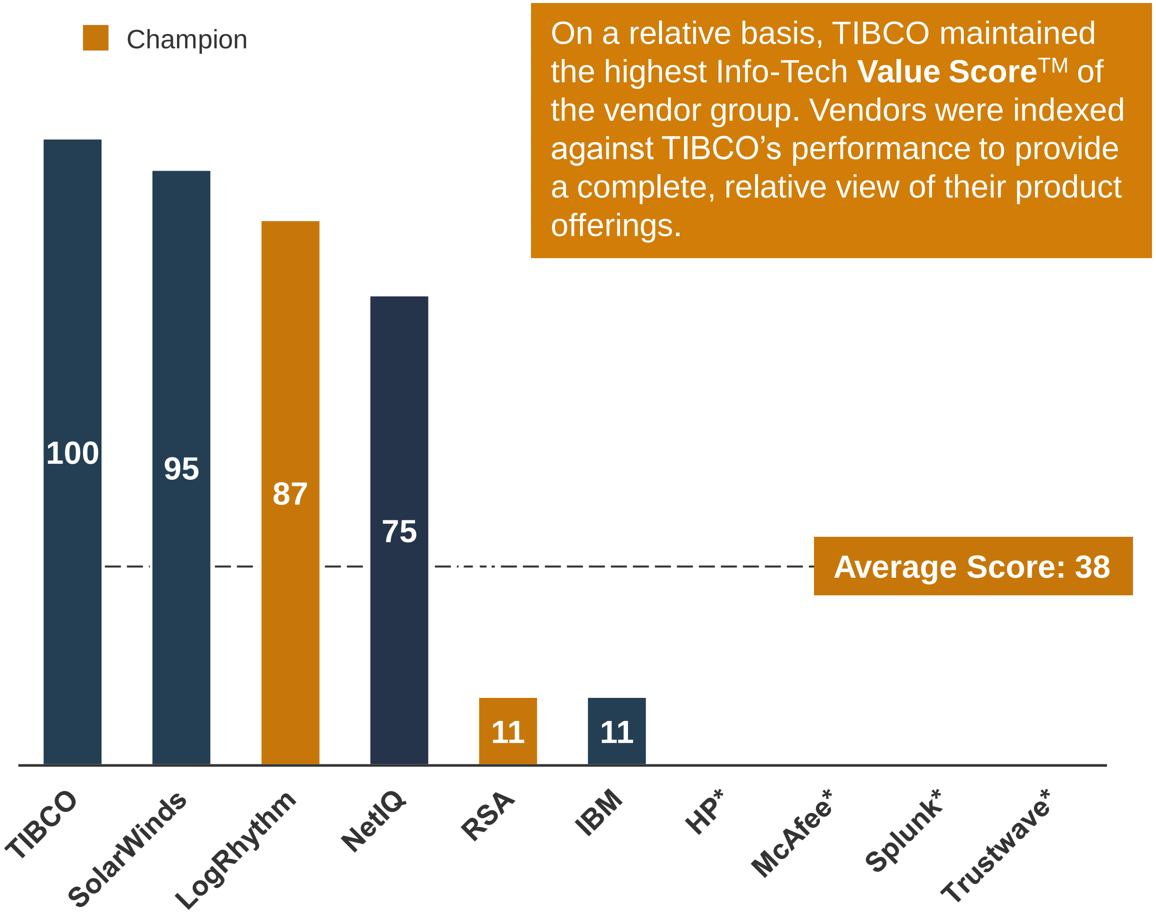
What is a Value Score?

The Value Score indexes each vendor's product offering and business strength **relative to its price point.** It **does not** indicate vendor ranking.

Vendors that score high offer more **bang-for-the-buck** (e.g. features, usability, stability, etc.) than the average vendor, while the inverse is true for those that score lower.

Price-conscious enterprises may wish to give the Value Score more consideration than those who are more focused on specific vendor/product attributes.

*The vendor declined to provide pricing and publicly available pricing could not be found.



On a relative basis, TIBCO maintained the highest Info-Tech **Value Score**^{TM} of the vendor group. Vendors were indexed against TIBCO's performance to provide a complete, relative view of their product offerings.

For an explanation of how Price is determined, see Information Presentation – Price Evaluation in the Appendix.

For an explanation of how the Info-Tech Value Index is calculated, see Information Presentation – Value Index in the Appendix.

Table Stakes represent the minimum standard; without these, a product doesn’t even get reviewed

The Table Stakes

Feature	What it is:
Basic Collection, Aggregation, Normalization (CAN)	Collection from firewall and network logs, IDS logs, Windows server logs, web server logs, and various *syslog* sources.
Basic Correlations	Out-of-the-box correlation policies for basic CAN data, acting in near real time.
Basic Alerting	Logging for all correlated events and alerting via pager/email/text for those that exceed a given threshold or meet specific alert criteria.
Basic Reporting	Availability of a variety of out-of-the-box reports that can be run on a scheduled and ad hoc basis.

What does this mean?

The products assessed in this Vendor Landscape$^{\text{TM}}$ meet, at the very least, the requirements outlined as Table Stakes.

Many of the vendors go above and beyond the outlined Table Stakes, some even do so in multiple categories. This section aims to highlight the products’ capabilities **in excess** of the criteria listed here.

Info-Tech Insight

If Table Stakes are all you need from your SIEM solution, the only true differentiator for the organization is price. Otherwise, dig deeper to find the best price to value for your needs.

Advanced Features are the capabilities that allow for granular market differentiation

Scoring Methodology

Info-Tech scored each vendor's features offering as a summation of its individual scores across the listed advanced features. Vendors were given one point for each feature the product inherently provided. Some categories were scored on a more granular scale with vendors receiving half points.

Advanced Features

Feature	What we looked for:
Log Data Enrichment	Advanced CAN from net flow, identity, database, application, configuration and file integrity data sources.
Advanced Correlation	Advanced canned policies, user-defined policies, adaptive/heuristic policies, and host criticality information inclusion.
Advanced Alerting	Programmable/customizable alerting responses and injection into native or third-party workflow tools.
Advanced Reporting	Flexible dashboards, custom and compliance reporting capabilities, and ability to export to external reporting infrastructure.
Forensic Analysis Support	Ability to generate custom data queries through flexible drill-down capabilities and export functions.
Data Management Security	Granular access controls to system and log data, encryption of SIEM data (in storage and transmission).

For an explanation of how Advanced Features are determined, see Information Presentation – Feature Ranks (Stoplights) in the Appendix.

Advanced Features are the capabilities that allow for granular market differentiation

Scoring Methodology

Info-Tech scored each vendor's features offering as a summation of its individual scores across the listed advanced features. Vendors were given one point for each feature the product inherently provided. Some categories were scored on a more granular scale with vendors receiving half points.

Advanced Features (Continued)

Feature	What we looked for:
Data Management Retention	Notable storage capacity, data compression, and inherent hierarchical storage management with integration capabilities.
Unified Compliance Framework	Solution leverages the UCF to enable advanced compliance reporting.
Threat Intelligence Feed	Vendor-provided security threat intelligence feed.
Automated Remediation	Bi-directional communication with network and security devices to enable automated remediation in face of defined incidents.

For an explanation of how Advanced Features are determined, see Information Presentation – Feature Ranks (Stoplights) in the Appendix.

Each vendor offers a different feature set; concentrate on what your organization needs

Evaluated Features

	Log Data Enrichment	Advanced Correlation	Advanced Alerting	Advanced Reporting	Forensic Analysis Support	Data Management Security	Data Management Retention	Unified Compliance Framework	Threat Intelligence Feed	Automated Remediation
HP	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢
IBM	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🔴
LogRhythm	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢
McAfee	🟢	🟢	🟢	🟢	🟡	🟡	🟡	🟢	🟢	🟡
NetIQ	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟡	🟢
RSA	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴
SolarWinds	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟡
Splunk	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🟢	🟡
TIBCO	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🔴	🔴	🔴
Trustwave	🟢	🟢	🟢	🟢	🟡	🟡	🟡	🔴	🟢	🔴

Legend 🟢 **=Feature fully present** 🟡 **=Feature partially present/pending** 🔴 **=Feature absent**

For an explanation of how Advanced Features are determined, see Information Presentation – Feature Ranks (Stoplights) in the Appendix.

Streamline monitoring, alerting, and incident response processes to minimize the cost of individual security events

Security event management relies on strong correlation and deep forensic analysis.

1 Management of Security Events

2

3

Why Scenarios?

In reviewing the products included in each Vendor Landscape™, certain use cases come to the forefront. Whether those use cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use cases as Scenarios, and calls attention to them where they exist.

Exemplary Performers

NetIQ.

NetIQ Sentinel automatically identifies and alerts on anomalous activity based on aggregated and consolidated enriched data. Correlation rules are associated with various actions including data forwarding to decrease response time.

RSA SECURITY

RSA Security Analytics contains powerful event stream analytics that support large data volumes with malware and network behavior analytics. Both real-time and long-term data collection and correlation are leveraged with complex event processing.

solarwinds

SolarWinds LEM employs a patented real-time, in-memory, non-linear analysis model that reduces the number of rules and complexity required. Correlations are supported by true field-level analysis, multiple decision paths, and independent thresholds.

For an explanation of how Scenarios are determined, see Information Presentation – Scenarios in the Appendix.

Reduce the cost of demonstrating regulatory and policy compliance by simplifying reporting and log review functions

Compliance capabilities are defined by broad and deep reporting.

1

2 Reduction of Compliance Complexity

3

Why Scenarios?

In reviewing the products included in each Vendor Landscape™, certain use cases come to the forefront. Whether those use cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use cases as Scenarios, and calls attention to them where they exist.

Exemplary Performers

NetIQ

NetIQ Sentinel comes with predefined regulatory reports enabling simplified collection of IT infrastructure events. Automated compliance audit and reporting functions reduce the complexity of locating and preparing data required by auditors.

RSA SECURITY

RSA Security Analytics provides compliance and trend reporting in an automated process. Support for long-term forensic analysis provides full incident investigation. Two-way integration with RSA Archer, Governance, Risk, and Compliance (GRC) is available.

solarwinds

SolarWinds LEM includes a standalone historical and compliance reporting console with predefined reports that are customizable. Customers can make an archive of event data that is encrypted and exportable via reports or a historical search.

LogRhythm

LogRhythm comes with pre-defined and customizable reports with direct integration with commercial reporting platforms. Drill-down pivot analysis, role-based access controls, and indexed data tier architecture all support compliance needs.

For an explanation of how Scenarios are determined, see Information Presentation – Scenarios in the Appendix.

Ensure the reduction of enterprise risk by putting broad-based collection, aggregation, and response abilities to good use

The broadest possible feature-functionality is required for true risk reduction.

1

2

3 Enhancement of Overall Risk Management

Why Scenarios?

In reviewing the products included in each Vendor Landscape^{TM}, certain use cases come to the forefront. Whether those use cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use cases as Scenarios, and calls attention to them where they exist.

Exemplary Performers

ArcSight ESM maps business indicators to IT assets and security events providing threat insight. Threat intelligence is layered onto network flow analysis to filter out malicious communication. Behavior-based pattern detection identifies advanced adversaries.

LogRhythm's AI Engine delivers heuristic correlation through advanced correlation, machine-automated behavioral analysis, and pattern recognition on all collected data. Behavioral Anomaly Detection and Privileged User Monitoring are some available rules.

NetIQ Sentinel acts as an aggregator and consolidator of enriched data to perform real-time correlation and event management. Log encryption, file integrity monitoring for host systems, change detection, and agent-based monitoring all enhance risk management.

RSA Security Analytics provides advanced reporting with cutting edge pre-defined reports. Pivot capabilities on terabytes of data is done in real time to enable free-form contextual analysis. Massive parallel infrastructure enables advanced query analysis.

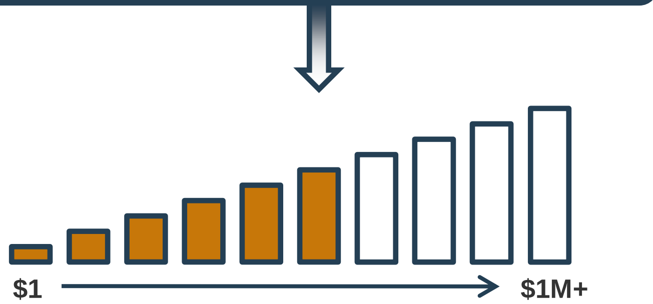
For an explanation of how Scenarios are determined, see Information Presentation – Scenarios in the Appendix.

LogRhythm, one of the few remaining dedicated SIEM vendors, is adaptable to the threat landscape

Champion

Product:	LogRhythm SIEM Version 6.2
Employees:	300
Headquarters:	Boulder, CO
Website:	logrhythm.com
Founded:	2003
Presence:	Privately Held

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000



Pricing provided by vendor

Overview

- LogRhythm is a SIEM dedicated security vendor. It delivers a strong SIEM product with built-in file integrity monitoring and host intrusion detection capabilities. Its modular platform offers flexibility and should be on the shortlist of companies of all sizes.

Strengths

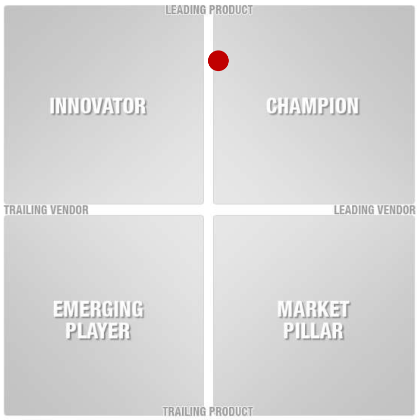
- LogRhythm uniquely combines enterprise-class SIEM, log management, file integrity monitoring, and machine analytics, with host and network forensics, in a unified security analytics platform.
- LogRhythm's machine analytics are powered by an AI engine that analyzes data in real time, identifying priority events providing advanced behavioral and statistical analysis.
- Ease of use when deploying and implementing as well as during performance management ensures strong value add.
- Integrated FIM secures sensitive data for compliance needs.

Challenges

- Due to its size, and in light of recent market movements, the possibility of LogRhythm being acquired must be considered even in the face of LogRhythm's acquisition-averse standing.
- Though an automated response can be configured, those customers that wish to manually approve and initiate SmartResponse tasks will have to log into the system to initiate an authorization process of up to three-steps. Future versions will allow for emailed responses instead.

The ability to dedicate itself has awarded LogRhythm one of the strongest advanced feature offerings within this VL

Vendor Landscape

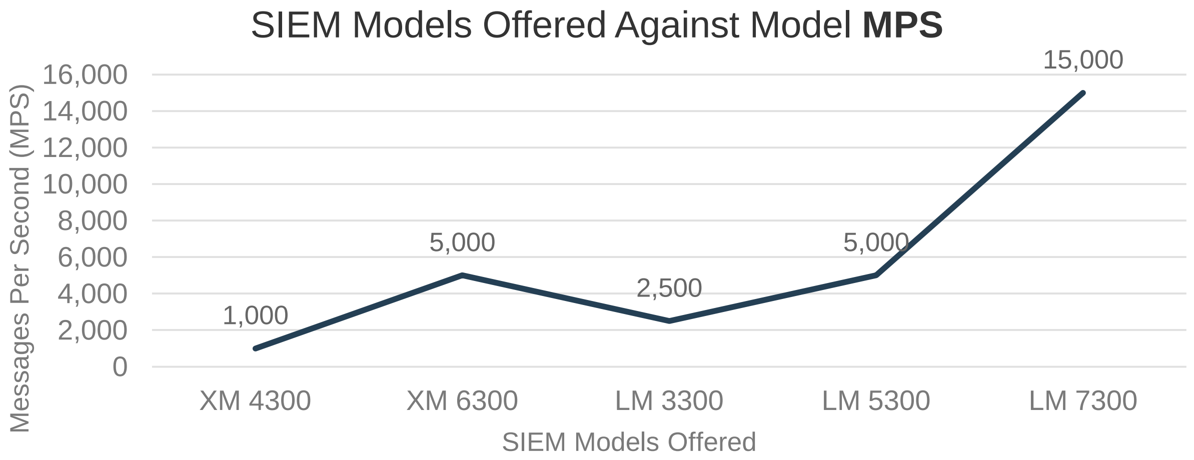


Value Index

87

3rd out of 10

Product					Vendor				
Overall	Features	Usability	Afford.	Arch.	Overall	Viability	Strategy	Reach	Channel
●	●	●	◕	●	◕	◕	●	◕	◕


SIEM Models Offered Against Model **MPS**

Features

Log Data Enrichment	Advanced Correlation	Advanced Alerting	Advanced Reporting	Forensic Analysis Support	Data Management Security	Data Management Retention	Unified Compliance Framework	Threat Intelligence Feed	Automated Remediation
🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢

Info-Tech Recommends:

LogRhythm's SIEM solution offers both administrator and end-user ease of use and strong feature-functionality. Users getting started with SIEM will appreciate its many features and uncomplicated installation. Calculate in the market trends of vendor consolidation when evaluating a dedicated SIEM vendor and its ability to stay independent or its value of providing single product lines.